AN INTRODUCTION TO THE P-23 CLASSIFIED COMPUTING FACILITY (P23SECURE)

AND

Rules of Use for P23SECURE

1. Scope

The P23SECURE local classified computing system is comprised of UNIX, LINUX and PC computers connected to the Protected Transmission Systems (PTS). The guidelines and rules outlined here apply to all of the computers within the P23SECURE system. Systems accredited under this plan are for classified computing only. *Also, throughout this document, the user interface device may be referred to as a* ***workstation*** *but it may actually be a terminal, printer, a PC, or other equivalent unit.*

2. Access and Passwords

Minimum clearance level for users accessing P23SECURE is a DOE Q clearance. A 'need to know' requirement is also applied to all users.

Passwords for signing on to this system will be classified Secret. Documents containing classified passwords will be marked and protected appropriately. Passwords will not be shared and users are forbidden to store passwords on-line. Failure to protect a password may result in a security infraction.

3. Logging on to the System

Each user of this system is assigned a unique username and unique password that is generated either by the ICN Password Office or by the crypto card. The user’s password and ID (username) will serve to authenticate the user to the system. The system stores sign-on passwords in encrypted form and allows a user two incorrect sign-on attempts. After the third incorrect sign-on attempt, the user account is blocked and prohibited from logging on to the system. The user must then contact the ISSO to be reinstated.

After a successful logon, when the operating system permits, each initial screen will contain a warning text to the user, who is required to take positive action to remove the notice from the screen.

4. P23SECURE LAN SOP and Workstation Signs

A copy of the P23SECURE LAN SOP will be posted near every workstation. The workstations, terminals, and other components will be conspicuously labeled with tape as SRD.

5. Fraud, Waste, and Abuse Auditing

The P-23 computers are intended for official laboratory business, not home budgets or personal mailing lists or such. If misuse is found or suspected, the user’s line manager will be notified. If warranted, S-Division staff and the Internal Evaluations Group AA-4 will also be notified.

6. Protected Transmission System (PTS)

A Protected Outlet Box (POB) will be installed for each workstation or KVM extender located outside of the vault. Each POB will be secured by a controlled access core and key that not only controls access to the POB, but, for emanations reasons, terminates the circuit in its typical (characteristic) impedance when the door is closed and locked.

You must follow official Laboratory policy in attending/securing a POB. Protect the lock box key from loss. Loss of a key will cause the recoring of all the locks in that series (usually all the lock boxes in the wing).

7. Output Marking

No software is available for this system to provide the users with the capability to put classification markings on their output automatically. **The responsibility for the proper marking, logging, handling, storing and destroying of all user-generated output rests with the individual user**. This includes ribbons used for classified printing.

The appropriate rubber stamps, pads, etc. will be provided in the facility. The ISSO or the Classified Media Custodian (CMC) will instruct personnel handling classified data to apply the appropriate markings to output. Users will follow procedures set by the organization's CMC to ensure that documents are marked and handled in accordance with LANL Office Procedures Manual.

Any output that remains in the computer room will be the responsibility of the ISSO and will be protected as SECRET RD until the proper classification level of the output has been determined. Unclaimed output that is over a week old will be destroyed in accordance with Laboratory procedures for destruction of classified documents.

8. Backups of the System

It is the users' responsibility to backup their data to the server(s). System backups will be done frequently. All data on the server will be backed up to electronic media. Storage for data and system backups will be in the P23SECURE vault-type-room. Off-site storage for data and system backups will be in a secure area at TA-3 SM216 (Group P-22.)

9. PC's

Owners/users of workstations are responsible to have them approved for operation prior to connecting them to the P23SECURE. Contact the ISSO for information on how to get approval.

10. User Workstations

Workstations will be located exclusively within the security area. They can either be in the VTR or in a user's office. No removable media (other than hard disks and read-only CD ROM) are allowed for systems outside of the VTR. This includes floppies, JAZ, ZIP, tape, etc.,

Monitors will be positioned to discourage unauthorized visual access. Workstations will be at least 6 inches from any unclassified resource that communicates via unprotected media (telephones, microcomputers with telephone modems, etc.).

Any workstations outside of the vault will be sanitized after each classified computing session. Sanitization procedures are included in the P23SECURE LAN Access SOP.

When workstations are unattended, the user will be responsible for ensuring that no classified data is accessible. This will be done by:

i. Logging off the system or activate the screen saver in case of the KVM extenders,
ii. Powering down the equipment if it is not a KVM extender,
iii. Locking the POB,
iv. Removing the controlled access key, and
v. Lock removable hard disk(s) in a GSA-approved safe.

I have read and understood and will follow the P23SECURE rules and guidelines.

Name:(print please)____

Z-Number:____

Signature:____

Date:____

POST NEXT TO YOUR PC OR WORKSTATION

P23SECURE LAN ACCESS

SOP

This is a Description of the method to connect and disconnect from P23SECURE LAN.

To connect:

1. Make sure all equipment to be used for classified access is of a minimum 6 inches from all other telecommunication equipment (phone, unclassified computers, etc.). The minimum separation between cables of classified and unclassified computers is 2 inches.
2. Close the window blinds and, if necessary, also the door to prevent viewing from unauthorized personnel.
3. Open the secure LAN lock box and plug in the network cable.
4. *****Take the classified boot disk out of your safe and insert it into your machine.
5. Turn on and boot your system.
6. Any printout from a classified computing session should be reviewed by an ADC (who may not be the same person as the user) and marked immediately according to the classification level.

To Disconnect:

1. *****Remove the classified boot disk(s) from the system and lock it in a safe.
2. *****Turn off your machine and all peripherals.
3. Disconnect from the secure LAN box and lock up the box.
4. If the system connects to a laser printer, at the end of a classified computing session, make sure that there is no unfinished printing job or paper jam. Then turn off the printer along with all other equipment for at least one minute.

***** If applicable

POST NEXT TO YOUR PC OR WORKSTATION